Remarks

Status of application

Claims 1-70 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

The invention

A system and methodology for protecting new computers by applying a preconfigured security update policy is described. In one embodiment, for example, a method of the present invention is described for controlling connections to a computer upon its initial deployment, the method comprises steps of: upon initial deployment of the computer, applying a preconfigured security policy that establishes a restricted zone of preapproved hosts that the computer may connect to upon its initial deployment; receiving a request for a connection from the computer to a particular host; based on the preconfigured security policy, determining whether the particular host is within the restricted zone of preapproved hosts; and blocking the connection if the particular host is not within the restricted zone of preapproved hosts.

General

The claims have been amended pursuant to the readability suggestions of the Examiner.

Prior art rejections

A. Section 102 rejection: Freund

Claims 1-4, 8-19, 22-29, 33-44, 47-52, 56-67 and 70 stand rejected under 35 U.S.C. 102(b) as being anticipated by Freund (US 5,987,611). Here, the Examiner has likened Applicant's claimed invention to Applicant's own prior patent. The claims have been amended to prevent such an interpretation.

To be sure, the underlying endpoint security system (commercial product of ZoneAlarm®), which is the subject of the' 611 patent, is used as part of the embodiment of the present invention. However, an important distinction exists. The original

ZoneAlarm® Security Suite product (as well as all other security products, including Norton, McAfee, etc.) have no notion of a "pre-access" firewall and access rules that limit a machine at the system level to only accessing specific sites (i.e., sites that the manufacture is aware of at the time that the image is built). In this manner, each machine receiving that configuration (disk image) will be limited to only contacting a limited set of security-relevant sites (i.e., pre-access restricted zone). Importantly, all other attempted connections to the machine (i.e., from non-approved addresses) are refused during the pre- and peri-access stage. Only upon a given machine completing updating of security subsystems is the machine's security policy updated to allow other connections to occur. In particular, until the machine has updated relevant security components, the machine is not allowed to participate with general connectivity to the Internet, and the user is informed that is unsafe to do so until the security-relevant updates have been completed. Quite simply, prior art versions of security software simply gave machines general connectivity to the Internet and provided firewall and antivirus protection with versions (and definition files) that were effectively guaranteed to be out-of-date by the time the machines reached consumer hands.

In accordance with the present invention, a new zone is introduced: a "restricted" zone (or "pre-access restricted zone") specifically for a new machine. Since the new machine operates in a restricted zone upon the initial deployment, the machine initially <u>cannot</u> be remotely accessed by another computer (e.g., a computer which is connected via a LAN or WAN). This restriction specifically addresses hacker probes, such as the MS-Blast worm (where infection can occur by virtue of a machine simply having Internet connectivity).

In order to bring these distinctions to the forefront, Applicant's claims have been amended to emphasize that the present invention is directed to enforcing pre-access connectivity restrictions on a new machine and emphasize that a "security <u>update</u> policy" is applied during this restricted access stage. For example, Applicant's independent claims have been amended to recite that "the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed." Here, the machine is restricted to only allow certain applications resident on the machine to connect to specific security-relevant sites that are specified in the security update policy (i.e., pre-access restricted zone). All other connections (e.g., from non-approved applications or processes, and/or to non-approved destinations) are denied. In other words, the user is effectively forced to apply relevant security updates before the machine is given general connectivity to the Internet. Importantly during this time, the machine simply cannot be infected (e.g., by a hacker scanning for an open port) since -- by default -- all other connections are denied. It is respectfully submitted that prior art versions of security software (including Applicant's prior version of ZoneAlarm®, which is the subject of the' 611 patent) simply did not function in that manner and thus do not provide an adequate basis of prior art to anticipate Applicant's claimed invention.

In view of the amendments to the claims and the remarks made above, it is respectfully submitted that the claims set forth a patentable advance over the art, and that any rejection under Section 102 is overcome.

B. Section 103 rejection: Freund and Perkins

Claims 5-6, 30-31 and 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund (US 5,987,611) in view of Perkins et al. (US 2004/0187028 A1). Here, the Examiner repeats the rejection based on the Freund above, but adds Perkins for the contention that it teaches the claim limitation of "wherein said preconfigured security update policy operates to prevent the computer from being remotely accessed by another computer upon the initial deployment." The claims are believed to be allowable for at least the reasons cited above pertain to the Section 102 rejection. Parkins itself includes no teaching overcoming this deficiency.

As stated above, Applicant's independent claims have been amended to emphasize that a "security update policy" is applied during this restricted access stage, for limiting the computer's connectivity. Importantly, the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed. As none of the prior art systems (including Applicant's own' 611 patent) functioned in that manner, it is respectfully submitted that those systems do not provide an adequate basis of prior art to teach or suggest Applicant's claimed invention, or render Applicant's invention obvious in view of Perkins. Therefore, it is respectfully submitted that the amended claims distinguish over the art and that any rejection under Section 103 is overcome.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: August 6, 2007

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX